

PATENT OFFICE  
JAPANESE GOVERNMENT



This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application: May 17, 2000

Application Number: Patent Application  
No. 2000-145274

Applicant(s): YAZAKI CORPORATION  
Micro-Technology Corporation

March 2, 2001

Commissioner,  
Patent Office Kouzou OIKAWA

Number of Certificate: 2001-3014267

日 本 国 特 許 庁

PATENT OFFICE  
JAPANESE GOVERNMENT

1100a U.S. PTO  
09/855798  
09/16/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日  
Date of Application:

2000年 5月17日

出 願 番 号  
Application Number:

特願2000-145274

出 願 人  
Applicant(s):

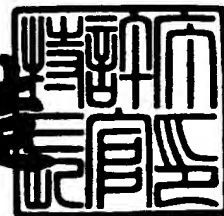
矢崎総業株式会社  
マイクロテクノロジー株式会社

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2001年 3月 2日

特 許 庁 長 官  
Commissioner,  
Patent Office

及 川 耕 造



出証番号 出証特2001-3014267

【書類名】 特許願

【整理番号】 YZK-4582

【提出日】 平成12年 5月17日

【あて先】 特許庁長官殿

【国際特許分類】 H03B 29/00  
G09C 1/00  
H01L 29/78

【発明の名称】 カオス暗号通信方法、及びカオス暗号通信システム

【請求項の数】 5

【発明者】

    【住所又は居所】 静岡県裾野市御宿 1 5 0 0 矢崎総業株式会社内

    【氏名】 石原 鉄也

【発明者】

    【住所又は居所】 静岡県裾野市御宿 1 5 0 0 矢崎総業株式会社内

    【氏名】 阿部 考浩

【発明者】

    【住所又は居所】 神奈川県横浜市旭区白根 5 丁目 4 5 番 1 2 号

    【氏名】 庄野 克房

【特許出願人】

    【識別番号】 000006895

    【氏名又は名称】 矢崎総業株式会社

    【代表者】 矢崎 裕彦

【特許出願人】

    【識別番号】 591235810

    【氏名又は名称】 マイクロテクノロジー株式会社

    【代表者】 山田 敬

【代理人】

    【識別番号】 100083806

    【弁理士】

【氏名又は名称】 三好 秀和

【電話番号】 03-3504-3075

【選任した代理人】

【識別番号】 100068342

【弁理士】

【氏名又は名称】 三好 保男

【選任した代理人】

【識別番号】 100100712

【弁理士】

【氏名又は名称】 岩▲崎▼ 幸邦

【選任した代理人】

【識別番号】 100087365

【弁理士】

【氏名又は名称】 栗原 彰

【選任した代理人】

【識別番号】 100079946

【弁理士】

【氏名又は名称】 横屋 赳夫

【選任した代理人】

【識別番号】 100100929

【弁理士】

【氏名又は名称】 川又 澄雄

【選任した代理人】

【識別番号】 100095500

【弁理士】

【氏名又は名称】 伊藤 正和

【選任した代理人】

【識別番号】 100101247

【弁理士】

【氏名又は名称】 高橋 俊一

【選任した代理人】

【識別番号】 100098327

【弁理士】

【氏名又は名称】 高松 俊雄

【手数料の表示】

【予納台帳番号】 001982

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9708734

【包括委任状番号】 9902582

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 カオス暗号通信方法、及びカオス暗号通信システム

【特許請求の範囲】

【請求項 1】 複数の CPU 間で通信線を介して情報の暗号通信を行う際に用いられる暗号通信方法において、

前記複数の CPU の各々に、カオス・ブロック暗号とカオス・ストリーム暗号を含む暗号アルゴリズムをそれぞれインストールしておき、

前記複数の CPU の各々は、これらの暗号アルゴリズムを組み合わせて情報の暗号通信を実行することを特徴とするカオス暗号通信方法。

【請求項 2】 複数の CPU 間を通信線を介して接続して構成され、これらの CPU 間で暗号通信を行う暗号通信システムにおいて、

前記複数の CPU の各々は、

秘匿対象となる平文コードを、カオス・ブロック暗号を用いて暗号化したあと、カオス・ストリーム暗号を用いて暗号化した暗号コードを送信する一方、

受信した暗号コードを、前記カオス・ストリーム暗号を用いて同期復元したあと、前記カオス・ブロック暗号を用いて復元したもとの平文コードを取得することを特徴とするカオス暗号通信システム。

【請求項 3】 複数の CPU 間を通信線を介して接続して構成され、これらの CPU 間で暗号通信を行う暗号通信システムにおいて、

前記複数の CPU の各々は、

秘匿対象となる平文コードを、カオス・ブロック暗号を用いて暗号化したあと、カオス・ストリーム暗号を用いて暗号化した暗号コードを送信する一方、

受信した暗号コードを、前記カオス・ストリーム暗号を用いて同期復元したあと、ブロック暗号鍵の照合を行い、正当なアクセスである旨が認証されたあと、前記カオス・ブロック暗号を用いて復元したもとの平文コードを取得することを特徴とするカオス暗号通信システム。

【請求項 4】 請求項 1 に記載のカオス暗号通信方法において、

前記カオス・ブロック暗号における暗号鍵、暗号表、復元表の各データベースを、適宜の初期値  $x(0)$  を与えることで一元管理することを特徴とするカオス暗号

通信方法。

【請求項5】 請求項2又は3に記載のカオス暗号通信システムにおいて、前記カオス・ブロック暗号における暗号鍵、暗号表、復元表の各データベースを、適宜の初期値 $x(0)$ を与えることで一元管理することを特徴とするカオス暗号通信システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、複数のCPU間で通信線を介して情報の暗号通信を行う際に用いられる暗号通信方法に係り、特に、不正なアクセスを防止して、正当なアクセスのみを保証する頑健かつ高い信頼性をもつ暗号通信を実現し得るカオス暗号通信方法、及びカオス暗号通信システムに関する。

【0002】

【従来の技術】

例えば、自動車・電車・航空機などの運輸産業の分野において、あらゆる外乱に対して頑健かつ高い信頼性をもつ社会システムの構築が強く要請されている。

【0003】

【発明が解決しようとする課題】

こうした要請に応えるために、比較的単純な一対一対応の論理演算処理や線形演算処理の結果をもとにしてシステムを構築することが考えられる。しかしながら、そうした思想をもとにシステムを構築したのでは、特に人命にかかわる産業においては、必ずしもその信頼性を十分に確保できないことが認識されている。

【0004】

ここで、デジタルコンピュータは2進コードの論理演算処理により、繰り返しの仕事をプログラムにしたがって忠実に実行するマシンである。大量のデータにでも対処できるため、システムに頑健性があるかのごとく信じられているが、基本的には一対一対応の論理演算処理マシンであるため、外乱に対してはきわめて弱い。コンピュータの暴走やウィルスによる汚染はその一つの例である。

【0005】

そこで、不正なアクセスを防止して、正当なアクセスのみを保証する頑健かつ高い信頼性をもつ実用的なシステムの構築が強く要請されていた。

## 【 0 0 0 6 】

本発明は、上述した実情に鑑みてなされたものであり、不正なアクセスを防止して、正当なアクセスのみを保証する頑健かつ高い信頼性をもつ暗号通信を実現し得るカオス暗号通信方法、及びカオス暗号通信システムを提供することを課題とする。

## 【 0 0 0 7 】

## 【課題を解決するための手段】

本発明の説明に先立って、本発明を想到するに至った経緯について言及する。家庭用電化製品における工業用汎用CPUの使い方と、今日の自動車・電車・航空機などの運輸産業の分野におけるCPUの使い方とは、基本的に同じである。同じ部品に、同じプログラムと同じデータベースを共通にインストールすれば、結果として同じ動作を繰り返すことは自明である。しかし、こうした使い方は、CPUが本来的にもつ高度な情報処理能力を十分に発揮しているとはいえない。

## 【 0 0 0 8 】

そこで、本発明者らは、不正なアクセスを防止し、正当なアクセスのみを保証することを主眼とした場合における、工業用汎用CPUの有効な使い方として、次の機能に着目した。すなわち、工業用汎用CPUのメモリには、PROM(programable read only memory)やEEPROM(electric elatable programable read only memory)などを搭載することができる。また、チップ毎にプログラムを変えることもできる。さらには、チップ毎にデータベースを変えることもできる。

## 【 0 0 0 9 】

こうした工業用汎用CPUがもつ資源を有効活用する観点から想到された請求項1の発明は、複数のCPU間で通信線を介して情報の暗号通信を行う際に用いられる暗号通信方法において、前記複数のCPUの各々に、カオス・ブロック暗号とカオス・ストリーム暗号を含む暗号アルゴリズムをそれぞれインストールしておき、前記複数のCPUの各々は、これらの暗号アルゴリズムを組み合わせ



情報の暗号通信を実行することを要旨とする。

【0010】

請求項1の発明では、複数のCPUの各々に、カオス・ブロック暗号とカオス・ストリーム暗号を含む暗号アルゴリズムをそれぞれインストールしておき、複数のCPUの各々は、これらの暗号アルゴリズムを組み合わせることで情報の暗号通信を実行する。結果として線形化されるように非線形量子化計測したカオスに基づき、カオス・ブロック暗号とカオス・ストリーム暗号が生成される。

【0011】

請求項1の発明によれば、カオス・ブロック暗号とカオス・ストリーム暗号の組み合わせに係る暗号アルゴリズムを複数の各CPUにそれぞれインストールし、そうした暗号アルゴリズムを用いて情報の暗号通信を実行することにより、頑健かつ高い信頼性をもつ暗号通信を実現し得るカオス暗号通信方法を提供することができる。

【0012】

一方、請求項2の発明は、複数のCPU間を通信線を介して接続して構成され、これらのCPU間で暗号通信を行う暗号通信システムにおいて、前記複数のCPUの各々は、秘匿対象となる平文コードを、カオス・ブロック暗号を用いて暗号化したあと、カオス・ストリーム暗号を用いて暗号化した暗号コードを送信する一方、受信した暗号コードを、前記カオス・ストリーム暗号を用いて同期復元したあと、前記カオス・ブロック暗号を用いて復元したもとの平文コードを取得することを要旨とする。

【0013】

請求項2の発明では、複数のCPUの各々は、秘匿対象となる平文コードを、カオス・ブロック暗号を用いて暗号化したあと、カオス・ストリーム暗号を用いて暗号化した暗号コードを送信する一方、受信した暗号コードを、前記カオス・ストリーム暗号を用いて同期復元したあと、前記カオス・ブロック暗号を用いて復元したもとの平文コードを取得する。

【0014】

また、請求項3の発明は、複数のCPU間を通信線を介して接続して構成され

、これらのCPU間で暗号通信を行う暗号通信システムにおいて、前記複数のCPUの各々は、秘匿対象となる平文コードを、カオス・ブロック暗号を用いて暗号化したあと、カオス・ストリーム暗号を用いて暗号化した暗号コードを送信する一方、受信した暗号コードを、前記カオス・ストリーム暗号を用いて同期復元したあと、ブロック暗号鍵の照合を行い、正当なアクセスである旨が認証されたあと、前記カオス・ブロック暗号を用いて復元したもとの平文コードを取得することを要旨とする。

## 【0015】

請求項3の発明では、複数のCPUの各々は、秘匿対象となる平文コードを、カオス・ブロック暗号を用いて暗号化したあと、カオス・ストリーム暗号を用いて暗号化した暗号コードを送信する一方、受信した暗号コードを、前記カオス・ストリーム暗号を用いて同期復元したあと、ブロック暗号鍵の照合を行い、正当なアクセスである旨が認証されたあと、前記カオス・ブロック暗号を用いて復元したもとの平文コードを取得する。

## 【0016】

ここで、カオス・ブロック暗号では、平文コードを例えば4ビットなどのブロック単位に分割し、別途用意した暗号鍵、暗号表、復元表をそれぞれ用いて、分割されたブロック単位で暗号化・復元を行う。カオス・ブロック暗号における暗号鍵は、ブロック単位毎に順番を与える整数列を、乱数を用いて生成したものである。暗号表は非線形量子化計測したカオスの過去のタイムシリーズである。復元表は暗号表を整理した対応関係表である。カオス・ブロック暗号の特徴は、暗号鍵を順列組み合わせで多数発行でき、暗号コードの復元に先立って暗号鍵の照合を行うことにより、正当なアクセスのみを保証できる点にある。送信データは暗号鍵と暗号コードである。送信データのうち、どこが暗号鍵であり、どこが暗号コードであるかが容易に知られないように、送信データにはあらかじめ転置・置換・反転などの、情報秘匿化を企図した基本操作を加えておく。

## 【0017】

カオス・ストリーム暗号では、非同期多重通信のためのPN(Pseud Noise:疑似雑音)信号として、カオスのタイムシリーズから切り出したカオス符号列を使

う。送受信を行う各CPUには同一のPN信号群をそれぞれインストールし、同期をとって送受信を行う。同期がとれないCPU間の送受信はすべて相互に雑音とみなされる。カオス・ストリーム暗号では、暗号コードは送信データたる平文コードとPN信号との排他的論理和演算（EXOR）をとって生成する。このときに信号の拡散を行っておくとよい。拡散をしてPN信号との排他的論理和をとったときには、再度PN信号とのEXORをとる復元のあとで拡散した部分の圧縮を行って、もとの平文コードに復元する。この過程で送信中の符号エラーを検証することができる。例えば車両のように雑音が多い環境下での暗号通信システムにおいては、エラー検証を自動的に包含するシステムの採用はきわめて重要といえる。

## 【0018】

本システムのCPUには、暗号表、復元表、暗号鍵、及びPN信号がインストールされる。暗号表、復元表はシステムに共通に与えられていてもよい。暗号鍵、PN信号、及び暗号コードを送受信する対になるCPUには、同じデータベースがインストールされる必要があるが、仕事の内容が異なるCPUには、異なるデータベースがインストールされる。

## 【0019】

原理的には、1本の通信線を共有し、複数のCPU間で非同期多重通信が実行される、共通鍵方式の暗号通信システムである。

## 【0020】

請求項2又は3の発明によれば、カオス・ブロック暗号とカオス・ストリーム暗号の組み合わせに係る暗号アルゴリズムを用いた暗号化・復元処理が施されるので、不正なアクセスを防止して、正当なアクセスのみを保証する頑健かつ高い信頼性をもつ暗号通信を実現し得るカオス暗号通信システムを構築することができる。これは、例えばPN信号が盗まれるような事態を生じた場合に、カオス・ストリーム暗号のみでは、暗号コードとPN信号との位相を相互にずらしてゆくことで原文を復元されてしまうのに対し、カオス・ブロック暗号とカオス・ストリーム暗号の組み合わせに係る暗号アルゴリズムを用いた暗号化・復元処理では、そうした事態を生じた場合であっても、あっさりと原文が復元されてしまうよ

うなことはなくなる事実由来している。

【0021】

また、請求項3の発明によれば、暗号コードの復元に先立って暗号鍵の照合を行うようにしたので、不正なアクセスを防止して、正当なアクセスのみを保証する頑健かつ高い信頼性をもつ暗号通信を実現し得るカオス暗号通信システムを構築することができる。

【0022】

ところで、機密性・公平性・公正性を厳格に要求する社会システムにおいて、こうしたシステムへの不正アクセスを防止し、正当なアクセスのみを保証する仕組みが強く要請されているのは既に述べた通りである。

【0023】

かかる要請に応える仕組みとして、従来、例えば、電子鍵、磁気カード、ICカードなどを活用した認証システムが導入されている。しかし、不正アクセスの防止を要求する社会システムの管理が、安易に人間に任されていることが多い。こうした場合、厳格に管理すべき人間の不正なアクセスが、社会システムの安全性を脅かしかねない。特に、暗号方式は人為的な取り決めに過ぎない以上、暗号鍵、暗号表、復元表の生成には人間の作為が関与せざるを得ない。したがって、そこにも人間による不正が入り込む余地を与えてしまう。

【0024】

こうした観点から、請求項4又は5の発明では、カオス・ブロック暗号において重要な役割を果たす、暗号鍵、暗号表、復元表の情報を、例えば52ビットの2進小数データなどの、最小の出発情報をもとに一元的に管理する手法を提案している。

【0025】

すなわち、請求項4の発明は、請求項1に記載のカオス暗号通信方法において、前記カオス・ブロック暗号における暗号鍵、暗号表、復元表の各データベースを、適宜の初期値 $x(0)$ を与えることで一元管理することを要旨とする。

【0026】

また、請求項5の発明は、請求項2又は3に記載のカオス暗号通信システムに

において、前記カオス・ブロック暗号における暗号鍵、暗号表、復元表の各データベースを、適宜の初期値 $x(0)$ を与えることで一元管理することを要旨とする。

【 0 0 2 7 】

カオスはそのタイムシリーズ  $\{y(t)-t\}$  のなかにあらゆる組み合わせを内包している。同相変換量子化したカオスのタイムシリーズは、その分解能に見合ったあらゆる整数の組み合わせを内包している。量子の縮退と過去への分岐を活用して、暗号表を設計したのがカオス・ブロック暗号である。暗号コードをもとの平文コードに復元する際に用いる復元表は、暗号表に従って従属的に作成される。

【 0 0 2 8 】

縮退した量子の箱と分割ブロックとの対応関係を整数の順列で定義し暗号鍵とする。カオス・ブロック暗号の構成要素である暗号鍵と暗号表は本来別々のものである。ところが、請求項 4 又は 5 の発明では、れらを別々のものとして取り扱わずに、共通の初期値 $x(0)$ から一元的に作成管理するようにしている。

【 0 0 2 9 】

請求項 4 又は 5 の発明によれば、カオス・ブロック暗号において重要な役割を果たす、暗号鍵、暗号表、復元表などを含む管理すべきシステム情報の量を低減することができる。また、人間が不正に関与する機会をできるだけ少なくして、人間が管理責任を問われることがないような社会システムの構築に寄与することができる。

【 0 0 3 0 】

【発明の実施の形態】

以下に、本発明に係るカオス暗号通信方法、及びカオス暗号通信システムの一実施形態について、図面を参照して説明する。

【 0 0 3 1 】

図 1 は、本発明に係るカオス暗号通信システムを、車載 CPU 間をデータ交換可能に接続して構成される車載通信システムに適用した例を示す。

【 0 0 3 2 】

同図に示すように、本発明に係るカオス暗号通信システムを構成する車載通信システム 11 は、例えばドアの内張内に設けられるドアロック制御用 CPU 13

と、例えばコンビネーションメータアッセンブリ内に設けられる情報表示用CPU15と、例えば運転席シートの下方に設けられるエンジン制御用CPU17と、これらCPU13, 15, 17の各間をデータ交換可能に接続する通信線19と、ドアロックアクチュエータ21と、コンビネーションメータ23と、を含んで構成されている。CPU13, 15, 17としては、例えば8ビットのものをを用いることができる。また、通信線19としては、ビットシリアルにデータ転送を行うときには1本の通信線を採用する一方、ビットパラレルにデータ転送を行うときには束ねられた通信線を採用するなど、データ転送方式などの実情に応じて適宜の態様のものを採用することができる。

## 【0033】

情報表示用CPU15には、自車の走行速度を計測する車速センサ（不図示）が接続され、また、エンジン制御用CPU17には、エンジンの回転速度を計測するエンジン回転速センサ（不図示）と、エンジン冷却水温を計測する冷却水温センサ（不図示）と、が接続されている。各種センサからの信号が入力として各CPU宛に取り込まれるにあたり、各種センサのアナログ信号はあらかじめAD変換される。このAD変換は線形である必要はない。特に、厳格な線形性を要求しない、例えばエンジン冷却水温などの種類の信号では、その重要性を考慮して非線形に重み付けしたAD変換を行うのが好ましい。そうした方が取り扱う情報量を減らすことができ、CPUの負担軽減が図れるだけでなく、技術を合理的にリストラしてシステムを再構成することができる。

## 【0034】

CPU13, 15に接続された外部のアクチュエータ21, 23の駆動を制御するために、DA変換処理を施して得られたアナログ信号を用いる。スイッチのオン・オフ制御はデジタル信号のままでよい。また、線形ではなく多段の設定制御を行うときには、4ビットまたは8ビットのデジタル信号で16段または256段までの多段制御が実現できる。DA変換も線形である必要はない。制御信号の重要性に応じた重み付けをしたDA変換が有効な場合も多い。なお、センサ側のAD変換を非線形にするか、アクチュエータ側のDA変換を非線形にするか、は必要に応じて適宜選択すればよい。両者共に非線形とする選択も考えられ

るが、そうすることの必然性がある訳ではない。

【 0 0 3 5 】

次に、上述の如く構成された本発明に係るカオス暗号通信システムを構成する車載通信システム 1 1 の動作を説明する。

【 0 0 3 6 】

まず、エンジン制御用 CPU 1 7 において、各種センサから入力される、回転速信号及び冷却水温信号の情報を含む平文コードに対し、ブロック暗号及びストリーム暗号を組み合わせた複合暗号アルゴリズムを用いて暗号化が施され、この暗号化で得られた暗号コードが、ある約束されたタイミングに従って通信線 1 9 に乗せられる。その暗号コードは情報表示制御用 CPU 1 5 により同期捕捉され、暗号化とは逆の過程をたどることでもとの平文コードたる回転速信号及び冷却水温信号の情報に復元されて、復元された情報がコンビネーションメータ 2 3 宛に送られる。このとき、ドアロック制御用 CPU 1 3 では、CPU 1 7 から送られてきた暗号コードは同期捕捉されない。CPU 1 3 からみると、CPU 1 7 から送られてきた回転速信号及び冷却水温信号の情報を含む暗号コードは単なる雑音に過ぎないからである。

【 0 0 3 7 】

また、情報表示制御用 CPU 1 5 において、車速センサから入力される車速信号の情報がコンビネーションメータ 2 3 宛に送られる一方、その情報を含む平文コードに対し、ブロック暗号及びストリーム暗号を組み合わせた複合暗号アルゴリズムを用いて暗号化が施され、この暗号化で得られた暗号コードが、ある約束されたタイミングに従って通信線 1 9 に乗せられる。その暗号コードはドアロック制御用 CPU 1 3 により同期捕捉され、暗号化とは逆の過程をたどることでもとの平文コードたる車速信号の情報に復元される。これを受けてドアロック制御用 CPU 1 3 は、復元された車速信号の情報などをもとに、ドアロックアクチュエータ 2 1 宛にドアロック信号を送る。これを受けてドアロックアクチュエータ 2 1 は、ドアロック状態を保持するように動作する。このとき、エンジン制御用 CPU 1 7 では、CPU 1 5 から送られてきた暗号コードは同期捕捉されない。CPU 1 7 からみると、CPU 1 5 から送られてきた車速信号の情報を含む暗号

コードは単なる雑音に過ぎないからである。

【0038】

このように、各CPU13, 15, 17に取り込まれた制御信号は、それぞれのCPUにインストールされたプログラムないしアルゴリズムに従って、信号を受け取り、符号化・多重化処理を行って通信線19宛に送り出される。この際、カオス・ストリーム暗号の同期捕捉を利用して信号の送受信が実行されている。すなわち、複数の車載CPUは時分割多重デジタル通信で制御されている。

【0039】

本発明にあっては、システムの更なる頑健性向上のために、カオス・ブロック暗号アルゴリズムを用いた暗号化が活用されている。カオス・ブロック暗号を用いた暗号化では、カオス符号列を用いて生成される暗号鍵が必要になる。暗号の復元に先立って、この暗号鍵を照合するようにシステムを構成すれば、ストリーム暗号の同期捕捉とのダブルチェックを実現可能である。

【0040】

カオス暗号化は、ブロック暗号に関しても、またストリーム暗号に関しても、MB/sオーダーの高速な処理速度を実現する。したがって、車両における情報処理では十分な処理速度であるといえる。CPUを介した通信は、車両への適用に限定されることなく、今日の産業を支える基本技術となりつつある。ノイズによる影響を含め誤った信号処理がシステムに被害を及ぼすことがないように、システムは構築されていなければならない。本発明はそのようなときに必要となる基幹技術である。

【0041】

本発明の結果、例えば車両の場合、同じ仕事を実行するのに、車両毎に異なる信号が使われることになる。例えばエンジンの点火タイミングを制御する信号は車両の走行状態を制御するための技術として重要な地位を占めているが、本発明では、そうした重要な信号が、ブロック暗号とストリーム暗号との組み合わせに係るカオス暗号アルゴリズムを用いて完全に秘話化されているため、例え第三者がその信号を盗み得たとしても内容が解読されることは起こり得ないという意味で、不正なアクセスを防止し、正当なアクセスのみを保証する頑健かつ高い信頼



性をもつ暗号通信を実現することができる。

【 0 0 4 2 】

また、複数の CPU にカオス暗号アルゴリズムを導入する本発明は、ブロック暗号とストリーム暗号との組み合わせに係る方式に適用できるというカオス技術がもつ暗号との親和性を活用することで、頑健性向上に寄与するダブルチェック機能をシステムに提供する。

【 0 0 4 3 】

さて、カオス・ブロック暗号において、暗号鍵・暗号表・復元表のもとになるカオス符号列を得る手段のひとつとして、次の例を挙げることができる。すなわち、

ディジタルコンピュータにおける仮数 5 2 ビットでの、

対称な非線形写像関数である

ロジスティックマップ  $x(t+1)=4x(t) \{1-x(t)\}$ 、

フィードバック  $x(t)=x(t+1)$ 、

同相変換量子化  $y(t)=[\{2/\pi \cdot \arcsin\sqrt{x(t)}\} \cdot 2^n]$ 、

(ただし、 $t$  は離散時間、 $x(t)$  は 0 と 1 の間に正規化された倍精度の実数で与えられるカオスの内部状態、 $[]$  は小数点以下を切り捨てる処理を意味する。)

の各計算式を与えておき、同相変換量子化  $y(t)=[\{2/\pi \cdot \arcsin\sqrt{x(t)}\} \cdot 2^n]$  を求める計算は、カオスのタイムシリーズ  $\{y(t)-t\}$  を得る有力な手段のひとつである。 $n=8$  としたときには、0 ～ 2 5 5 の整数のカオス的配列タイムシリーズである。計算の初期値  $x(0)$  は最小の出発情報 (5 2 ビット 2 進小数データ) で与えられる。

【 0 0 4 4 】

このタイムシリーズ上で  $y(t)$  と  $\tau$  ステップ過去の値  $y(t-\tau)$  との間には秩序立った分岐の関係にあり、 $2^\tau$  重の縮退 (退化) が生じている。タイムシリーズを検索して、各縮退した量子の箱に属する値  $y(t-\tau)$  を求め、これを暗号表とする。時間  $t$  の順序を入れ換えない限り、初期値敏感性は暗号表の中に残されている。

【 0 0 4 5 】

暗号鍵は、分割デジタルブロックと暗号表の縮退した量子の箱との対応である。これは、整数  $0, 1, 2, \dots, (2^{\tau} - 1)$  の順列で表される。 $\tau = 4$  とすれば、整数  $0 \sim 15$  の順列であり、その種類は  $16!$  通りとなる。

## 【0046】

暗号鍵たる  $0, 1, 2, \dots, (2^{\tau} - 1)$  の順列は、従来よく知られた疑似乱数生成方法によっても生成できるが、カオスのタイムシリーズから取得することもできる。カオスのタイムシリーズから取得する場合には、例えば、52ビット2進小数データである任意の初期値  $x(0)$  から繰り返し再生可能である。ひとつの初期値  $x(0)$  を、暗号鍵・暗号表・復元表の作成に共通に利用することにより、カオス・ブロック暗号において重要な役割を果たす暗号鍵・暗号表・復元表の一元管理が実現可能となる。

## 【0047】

カオスのタイムシリーズから暗号鍵たる  $0, 1, 2, \dots, (2^{\tau} - 1)$  の順列を取得するアルゴリズムはいくつも考えられる。例えば、同相変換量子化の分解能を  $n = 1$  とし、2進コード疑似乱数を生成し、 $\tau$  ビット毎に束ね、 $0 \sim (2^{\tau} - 1)$  の順列を取得することができる。また、同相変換量子化の分解能を  $n = \tau$  とし、 $0 \sim (2^{\tau} - 1)$  の順列を取得することもできる。

## 【0048】

具体的には、量子化分解能  $n = 8$ 、過去へ戻るステップ  $\tau = 4$  の例は、実用上手頃な実施例である。ワープロ平文文書は7ビットのアスキーコードで記述され、1文字当たり8ビット(1バイト)を単位として処理される。 $\tau = 4$  は4ビットブロックを意味し、端数を生じないカオス・ブロック暗号化復元処理を高速(例えば  $10\text{MB/s}$ ) に実行する。

## 【0049】

量子化分解能  $n = 8$  は、4ビットブロック平文コードが8ビット暗号コードに変換されることを意味する。従って、平文ファイルが2倍に拡張スクランブルされて暗号コードファイルとなる。平文ファイルにおける2値分布には、8ビット表記では筆頭ビットの値が常に「0」になるというアスキーコード固有の偏りがあるのに対し、暗号コードファイルではカオス特有の偏りのない2値分布となり

、このことから、暗号コードファイルをもとに平文ファイルを推測することは到底不可能であるといえる。

#### 【0050】

量子化分解能  $n = 8$ 、過去へ戻るステップ  $\tau = 4$  のとき、52ビット2進小数データたる任意の初期値  $x(0)$  からタイムシリーズ  $y(t)-t$  を計算する場合、タイムシリーズの長さ  $t_{\max} = 2^{16} = 65,536$  が適当である。縮退した16個の量子の箱には平均4,096個の8ビットコードが割り当てられ、逐次暗号コードとして提供される。

#### 【0051】

ひとつの初期値  $x(0)$  から  $n = 1$  として  $t_{\max} = 2^{16} = 65,536$  まで2進コード（疑似乱数列）を生成し、4ビット毎に区切って0～15の順列を暗号鍵として生成する。その数は1200本である。その中から任意に取り出した順列を組み合わせて暗号鍵とすると、組み合わせの総数は144万通りにもなる。なお、この組み合わせを利用して、暗号を階層的に構成することもできる。

#### 【0052】

取得された0～15の順列が、相互に十分離れた距離にあることは、相互相関を調べることによって検証することができる。

#### 【0053】

52ビット2進小数は、今日のデジタルコンピュータが計算可能な単位である。本発明では、そうした52ビット2進小数を初期値  $x(0)$  として、カオス・ブロック暗号を具現化する上で必要なデータベースの全てを一元管理することができる。

#### 【0054】

このように、本発明によれば、カオス・ブロック暗号を具現化する上で必要なデータベースの全てを、ひとつの初期値を出発点として一元管理するようにしたので、人間が関与する余地を極力減じて、人間が責任を問われることのない公平で安全な社会システムの構築に寄与するところ大である。

#### 【0055】

なお、上述した実施の形態は、本発明の理解を容易にするために例示的に記載

したものであって、本発明の技術的範囲を限定するために記載したものではない。すなわち、本発明は、その技術的範囲に属する全ての実施の形態を含むことは当然として、そのいかなる均等物をも含む趣旨である。

## 【 0 0 5 6 】

具体的には、例えば、上述した実施形態において、図 1 に示すように、複数の CPU を通信線を介して相互接続した形態を例示して説明したが、本発明はこの形態に限定されることなく、複数の CPU を例えば赤外線などの無線媒体を介して相互接続した形態をもその技術的範囲に含む。電波はあらゆる方向に放射される。目的とする CPU 以外でも当然に受信される。ストリーム暗号を用いた同期捕捉はそうした場面でも特に有効であることは言うまでもない。

## 【 0 0 5 7 】

## 【発明の効果】

以上説明したように、請求項 1 の発明によれば、カオス・ブロック暗号とカオス・ストリーム暗号の組み合わせに係る暗号アルゴリズムを複数の各 CPU にそれぞれインストールし、そうした暗号アルゴリズムを用いて情報の暗号通信を実行することにより、頑健かつ高い信頼性をもつ暗号通信を実現し得るカオス暗号通信方法を提供することができる。

## 【 0 0 5 8 】

請求項 2 又は 3 の発明によれば、カオス・ブロック暗号とカオス・ストリーム暗号の組み合わせに係る暗号アルゴリズムを用いた暗号化・復元処理が施されるので、不正なアクセスを防止して、正当なアクセスのみを保証する頑健かつ高い信頼性をもつ暗号通信を実現し得るカオス暗号通信システムを構築することができる。

## 【 0 0 5 9 】

また、請求項 3 の発明によれば、暗号コードの復元に先立って暗号鍵の照合を行うようにしたので、不正なアクセスを防止して、正当なアクセスのみを保証する頑健かつ高い信頼性をもつ暗号通信を実現し得るカオス暗号通信システムを構築することができる。

## 【 0 0 6 0 】

そして、請求項 4 又は 5 の発明によれば、カオス・ブロック暗号において重要な役割を果たす、暗号鍵、暗号表、復元表などを含む管理すべきシステム情報の量を低減することができる。また、人間が不正に関与する機会をできるだけ少なくして、人間が管理責任を問われることがないような社会システムの構築に寄与することができるといったきわめて優れた効果を奏する。

【図面の簡単な説明】

【図 1】

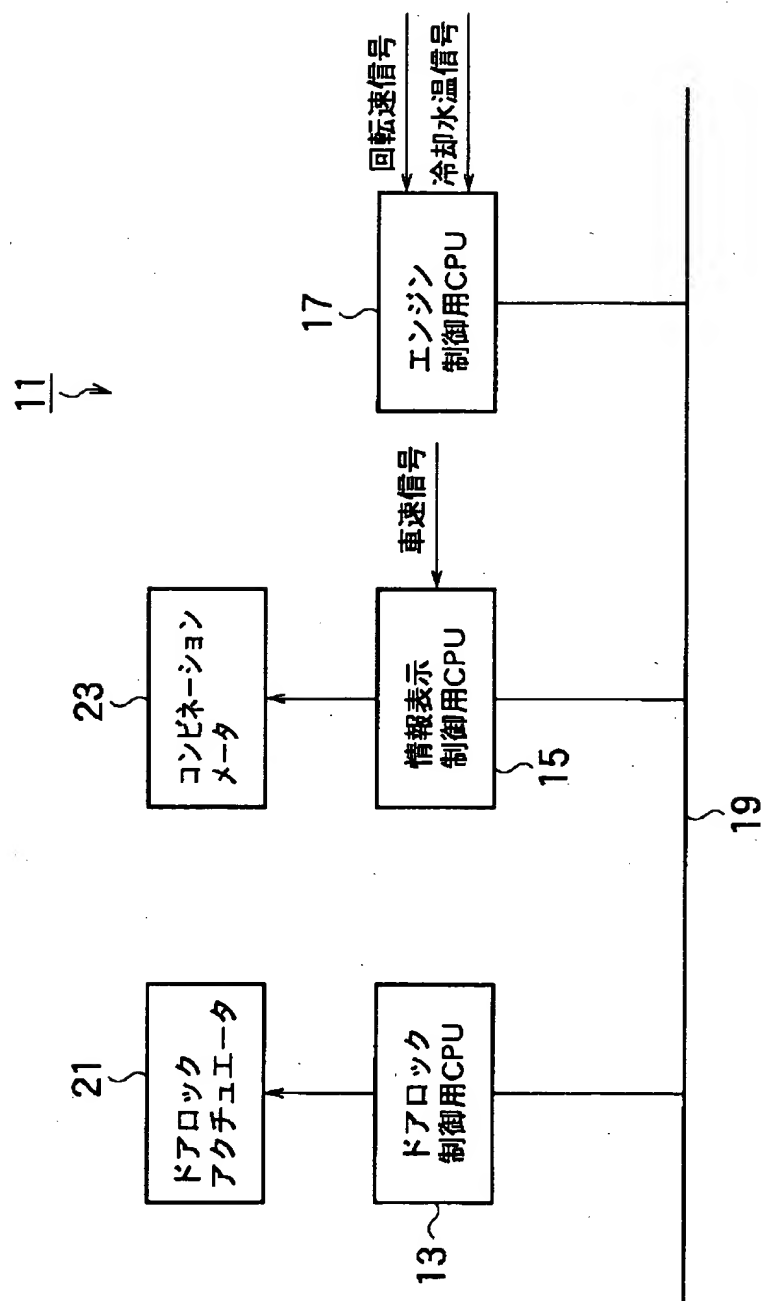
図 1 は、本発明に係るカオス暗号通信システムを、車載 CPU 間をデータ交換可能に接続して構成される車載通信システムに適用した例を示す図である。

【符号の説明】

- 1 1 車載通信システム（カオス暗号通信システム）
- 1 3 ドアロック制御用 CPU
- 1 5 情報表示制御用 CPU
- 1 7 エンジン制御用 CPU
- 1 9 通信線
- 2 1 ドアロックアクチュエータ
- 2 3 コンビネーションメータアッセンブリ

【書類名】 図面

【図 1】



【書類名】 要約書

【要約】

【課題】 不正なアクセスを防止して、正当なアクセスのみを保証する頑健かつ高い信頼性をもつ暗号通信を実現し得るカオス暗号通信方法、及びカオス暗号通信システムを提供することを課題とする。

【解決手段】 複数のCPU 13, 15, 17の各々は、秘匿対象となる平文コードを、カオス・ブロック暗号を用いて暗号化したあと、カオス・ストリーム暗号を用いて暗号化した暗号コードを通信線19を介して送信する一方、受信した暗号コードを、前記カオス・ストリーム暗号を用いて同期復元したあと、前記カオス・ブロック暗号を用いて復元したもとの平文コードを取得する。

【選択図】 図1

出 願 人 履 歴 情 報

識別番号 [000006895]

1. 変更年月日	1990年 9月 6日
[変更理由]	新規登録
住 所	東京都港区三田1丁目4番28号
氏 名	矢崎総業株式会社



出 願 人 履 歴 情 報

識別番号 [591235810]

1. 変更年月日 1994年 4月12日

[変更理由] 住所変更

住 所 東京都文京区大塚6丁目7番4-302号

氏 名 マイクロテクノロジー株式会社